

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

*LINES*

*Dots*

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-285283  
(43)Date of publication of application : 12.10.2001

(51)Int.Cl. H04L 9/32  
G09C 1/00  
H04L 9/08  
H04L 12/28  
H04L 12/66

(21)Application number : 2000-094840  
(22)Date of filing : 30.03.2000

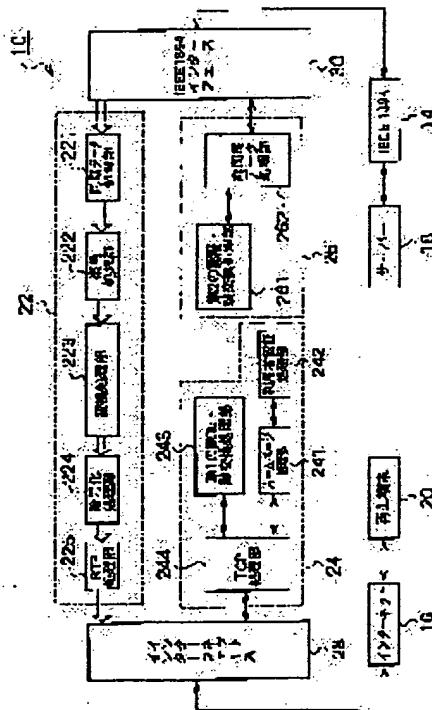
(71)Applicant : TOSHIBA CORP  
(72)Inventor : SAITO TAKESHI

## (54) COMMUNICATION UNIT AND ITS COMMUNICATION METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a communication unit that can realize protection of copyright in the case of transmitting data from a home network to a public network and to provide its communication method.

**SOLUTION:** The communication unit interconnects a public network 16 such as the Internet and a home network 14 such as a network in compliance with the IEEE 1394. This communication unit consists of a 1st authentication/key exchange processing section 243 that performs authentication/key exchange with a reproduction terminal 20 connected to the public network 16, a 2nd authentication/key exchange processing section 261 that performs authentication/ key exchange with a server 18 connected to the home network 14, a transmission section 22 that transmits AV data that are encrypted for copyright protection and obtained from the server 18 to the reproduction terminal 20, and a user authentication processing section 242 that authenticates a user of the reproduction terminal 20 and rejects communication with the reproduction terminal 20 when the user cannot be authenticated.



## LEGAL STATUS

[Date of request for examination] 20.09.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]



タ(AVデータ)を受信し、その受信されたAVデータを、たとえばエムペグ-4(MPEG-4)等に圧縮した後、インターネット側に送信する、という注目すべきアイディアがある。これは、外出先から、家庭内のAVコンテンツを閲覧可能にしたり、家庭内の監視カメラによって撮影されたAVデータを、家庭外から参照可能にする等、多くのアプリケーションが考えられるからである。

#### 【0004】

【発明が解決しようとする課題】ホームネットワーク上を流れるAVデータには、映画や音楽、音声、テレビ番組等、の著作物が含まれている場合がある。もちろん、AVデータ自身が著作物である場合もある。このような著作物を含む、あるいは著作物自体であるAVデータは、著作権による保護のため、ホームネットワーク上では暗号化されて送信される場合が多い。このため、ホームネットワーク上で入手された、暗号化AVデータをインターネットに再送信する場合、暗号化AVデータを一旦復号し、その暗号化を解除する必要がある。しかし、その復号されたAVデータをそのまま暗号化せずに、インターネット側に送信したのでは、今度は、インターネット上における著作権保護の意味が失われてしまうことになる。

【0005】一方、ホームゲートウェイが置かれている家庭の利用者以外からの、家庭内のAVコンテンツの閲覧・参照等の要求に対して、不用意に答えてしまうと、インターネットを介して不特定多数にコンテンツを送信してしまうことになりかねない。このことは、著作権法上で定められた「個人で楽しむ限りにおいては、タイムシフトや加工等が許される」という原則に反することになる。

【0006】このように、従来においては、ホームネットワークからインターネットに供給される著作物の送信については、著作権保護の観点からは、未だ不十分である。

【0007】本発明は、このような課題を解決し、家庭網から公衆網へデータを送信する際の著作権保護を実現する通信装置およびその通信方法を提供することを目的とする。

#### 【0008】

【課題を解決するための手段】上記課題を解決するため、本発明は、第1の網(公衆網)16と第2の網(家庭網、ローカルエリアネットワーク)14の間に配置され、公衆網16に接続された第1の端末(再生端末)20と家庭網14に接続された第2の端末(サーバー)18の間に暗号化データを転送する通信装置であることを特徴とする。

【0009】より詳細には、本発明の第1の特徴は、上記の通信装置であって、再生端末20との間で、認証・鍵交換を実行する第1の認証・鍵交換部243と、サーバー18との間で、認証・鍵交換を実行する第2の認証・鍵交換部261と、サーバー18から得られた暗号化

データに、所定の変換を施し、かつその暗号化データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、再生端末20に送信する送信部22と、再生端末20の利用者を認証し、その利用者の認証ができない場合には、再生端末20との通信を拒絶する利用者認証部242と、から構成される通信装置であることを第1の特徴とする。ここで、「暗号化データ」とは、少なくとも一部に著作物を含む、テキストや、写真、イラスト、絵画、アニメ、映画、音楽、音声、テレビ番組、WWWデータ等であって、著作権法による保護のために暗号化されているものである。

「所定の変換」とは、データ圧縮符号化方式およびデータ圧縮符号化速度のうちの少なくとも一方を変換することを意味する。より具体的には、家庭網14上を流れる暗号化データのデータ圧縮符号化方式、符号化速度を、公衆網16に適した符号化方式、符号化速度に、変換することである。「暗号制御情報」とは、サーバー18から得られたデータの録画やコピーを制御する情報である。たとえば、これ以上コピーを認めないという“No More Copy”である。

【0010】本発明の第1の特徴によれば、再生端末20の利用者を認証することで、サーバー18内のデータを要求する利用者が、正規の人物であることを十分に予想することができる。このため、利用者の認証以降の手順が、その利用者が個人的に楽しむための手順であることが明らかとなる。したがって、このことから、著作権法上で定められた「個人で楽しむ限りにおいては、タイムシフトや加工等が許される」という原則を遵守することが可能となる。

【0011】さらに、あらかじめ付加されていた、“No More Copy”等の暗号制御情報を、再生端末20に送信する際にも付加するので、元々のコピー制御の指定を守ることができる。このため、たとえば、録画やコピーをしてはいけない、と指定されていたデータは、再生端末20に送信する際も、録画やコピーを未然に防止する形式にできる。

【0012】本発明の第2の特徴は、上記の第1の特徴で述べた通信装置が実現する通信方法に係る。すなわち、第1の網(公衆網)16に接続された第1の端末(再生端末)20と第2の網(家庭網、ローカルエリアネットワーク)14に接続された第2の端末(サーバー)18との間で暗号化データを転送する通信方法であり、再生端末20の利用者を認証する工程と、その利用者の認証ができた場合のみ、サーバー18から暗号化データを取得する工程と、その取得された暗号化データに、所定の変換を施し、かつその暗号化データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、再生端末20に送信する工程と、少なくとも含む通信方法であることである。

#### 【0013】

と、復号処理部222と接続し、復号されたAVデータ(MPEG-2データ)をMPEG-2符号からMPEG-4符号に変換する変換処理部223と、変換処理部223と接続し、MPEG-4符号に変換されたAVデータ(MPEG-4データ)を、再び暗号化する暗号化処理部224と、暗号化処理部224と接続し、暗号化されたAVデータをリアルタイムに、インターネットインターフェース(以下、単に「インターネットI/F」と呼ぶ)28を介して、インターネット16側に送信するリアルタイムトランSPORTプロトコル(RTP)処理部225と、から構成される。

【0024】第1の認証・鍵交換部24は、インターネット16を介して、サーバー18内に蓄積された映像や音楽等のAVコンテンツの閲覧・参照等を要求する、各利用者の再生端末20に、識別ID(利用者ID)およびパスワード入力用ダイアログ画面を備えた利用者認証用ホームページおよびIEEE1394バス14に接続されたサーバー18や家電機器等を遠隔制御するため遠隔制御用ホームページを含む、各種のホームページを送信するホームページ処理部241と、利用者認証用ホームページのダイアログ画面から入力された利用者IDおよびパスワードが正規のものであるか否かを照合する利用者認証処理部242と、正規の利用者の再生端末20との間で認証・鍵交換処理を実行する第1の認証・鍵交換処理部243と、再生端末20とのやりとりをTCPパケット化するためのTCP処理部244と、から構成される。

【0025】第2の認証・鍵交換部26は、サーバー18との間で認証・鍵交換処理を実行する第2の認証・鍵交換処理部261と、サーバー18とのやりとりを非同期パケット化するための非同期データ処理部262と、から構成される。

【0026】次に、図3乃至図5を参照して、本発明の実施の形態に係る通信装置10の動作について説明する。図3は、本発明の実施の形態に係る通信装置10と、サーバー18および再生端末20との間の処理シーケンスチャートであり、図4および図5は、本発明の実施の形態に係る通信方法の処理手順を示すフローチャートである。

【0027】(1) 図3のステップS101において、まず、再生端末20が、インターネット16を介して、通信装置10に対して、サーバー18内のデータを閲覧・参照するための遠隔制御用ホームページを要求する(図4のステップS201)。この遠隔制御用ホームページには、IEEE1394バス14に接続された、サーバー18や各種の家電機器を遠隔制御するためのボタンが少なくとも表示される。このボタンは、たとえばグラフィカルユーザインターフェース(Graphical User Interface; GUI)で構成される。

【0028】(2) 図3のステップS102において、再生端末20からの遠隔制御用ホームページ要求を受けた通信装置10は、再生端末20に利用者認証用ホームページを送信し、利用者IDおよびパスワードを要求する(図4のステップS202)。

通信装置10は、この利用者IDおよびパスワードを要求し、ホームページを要求する再生端末20に利用者が、正規の利用者であるか否かを判断する。すなわち、要求されたホームページは、サーバー18や家電機器等の遠隔制御を可能とするものであり、正規の利用者以外にこのホームページを与えててしまうと、不審な人物にサーバー18や家電機器の制御をされかねない。そこで、通信装置10は、遠隔制御用ホームページを要求する再生端末20に対して、利用者IDおよびパスワードの入力を要求し、その利用者があらかじめ登録された、怪しくない人物であるか否かを確認する。

【0029】(3) 図3のステップS103において、利用者IDおよびパスワードの入力を要求された再生端末20の利用者は、たとえば再生端末20に設けられたダイヤルキーを用いて、利用者IDおよびパスワードを入力する。再生端末20に入力された利用者IDおよびパスワードは、インターネット16を経由して、通信装置10に送信される。

【0030】(4) 図3のステップS104において、再生端末20から送信された利用者IDおよびパスワードを受け取った通信装置10は、たとえば正規の利用者の利用者IDおよびパスワードを格納するデータベースを有している。そして、通信装置は、受け取った利用者IDおよびパスワードがそのデータベースに登録されているか否かを照合する(図4のステップS203)。利用者IDおよびパスワードが登録されていなければ(図4のステップS203NO)、直ちに、再生端末20との回線を切断する(図5のステップS204)。

【0031】(5) 利用者IDおよびパスワードが登録されている(図4のステップS203YES)、図3のステップS105において、通信装置10は遠隔制御用ホームページを、インターネット16を介して、再生端末20に送信する(図5のステップS205)。そして、再生端末20の利用者は、遠隔制御用ホームページに表示された、サーバー18の制御用ボタンを操作することで、たとえば図6に示すようなコンテンツ選択画面を取得する。図6に示すように、このコンテンツ選択画面32には、「ホームページに録画されている番組は以下の通りです。」と表示されており、利用者は、この選択画面32から、サーバー18内のコンテンツの再生が可能となる。すなわち、この選択画面32には、各コンテンツに対応付けられた、複数のボタン34(「ドラマ」34a、「スポーツ」34b、「ニュース」34c、「プライベートビデオ1」34d、「プライベートビデオ2」34e)が表示されており、各ボタン34を操作することで、各ボタン34に対応付けられたコンテンツを再生させることができる。

なお、遠隔制御用ホームページを取得した利用者は、その遠隔制御用ホームページを取得した利用者は、その遠隔制御用ホームページ

のAVデータを蓄積／コピーすることはできない。その場で、デコード／表示させることができるだけである。

【0042】このように、本発明の実施の形態によれば、家庭網上で入手された、チャンネル作物を含む、あるいは著作物自体のAVデータを、公衆網に送信する場合に、その著作物の著作権法による保護を確実に実現することができる。

【0043】特に、近年のデジタル化・ネットワーク化の進展により、ネットワーク上で著作物を送信するという著作物の利用方法が発達・普及する現状にあっては、本発明の重要性はきわめて高いものである。

【0044】  
【発明の効果】本発明によれば、家庭網から公衆網へ著作物を送信する際に、その著作物の保護を確実に実行する通信装置を実現できる。

【0045】本発明によれば、家庭網から公衆網へ著作物を送信する際に、その著作物の保護を確実に実行する通信方法を実現できる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態に係る通信装置によって接続された、家庭網と公衆網とからなるネットワーク・システムの全体構成を示すブロック図である。

【図2】本発明の実施の形態に係る通信装置の具体的な構成を示すブロック図である。

【図3】本発明の実施の形態に係る通信装置、サーバーおよび再生端末間で、著作物を含むAVデータを送受信する際の、処理シーケンスチャートである。

【図4】本発明の実施の形態に係る通信装置の通信方法の処理手順を示すフローチャートである（その1）。

【図5】本発明の実施の形態に係る通信装置の通信方法

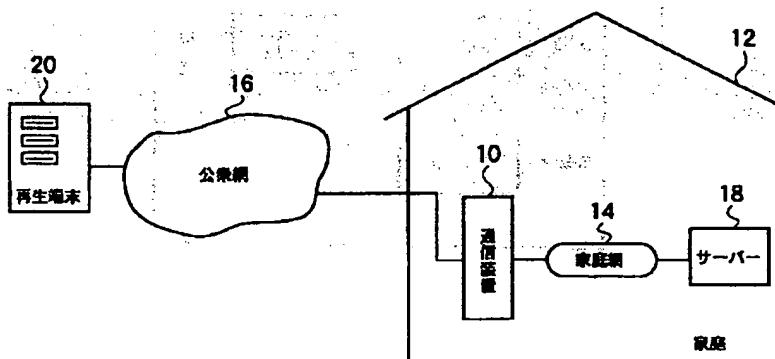
の処理手順を示すフローチャートである（その2）。

【図6】本発明の実施の形態に係る通信装置から、再生端末に送信される、コンテンツ選択画面の内容を示す図である。

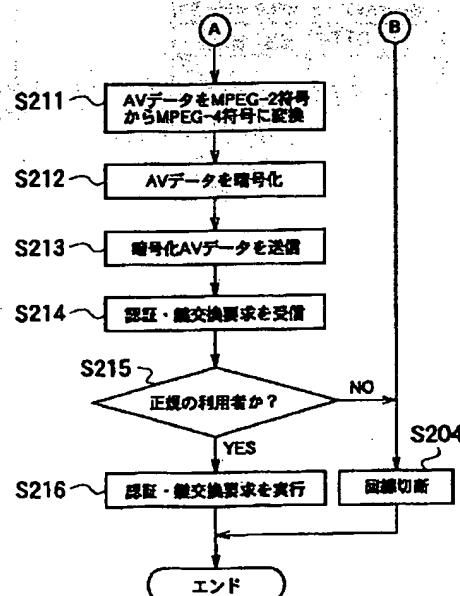
#### 【符号の説明】

- 10 通信装置
- 12 家庭
- 14 家庭網
- 16 公衆網
- 18 サーバー
- 20 再生端末
- 22 送信部
- 24 第1の認証・鍵交換部
- 26 第2の認証・鍵交換部
- 28 インターネットインターフェース
- 30 IEEE1394インターフェース
- 32 コンテンツ選択画面
- 34 ボタン
- 221 同期データ処理部
- 222 復号処理部
- 223 変換処理部
- 224 暗号化処理部
- 225 RTP処理部
- 241 ホームページ処理部
- 242 利用者認証処理部
- 243 第1の認証・鍵交換処理部
- 244 TCP処理部
- 261 第2の認証・鍵交換処理部
- 262 非同期データ処理部

【図1】



【図5】



フロントページの続き

F ターム(参考) 5J104 AA07 AA13 BA02 EA04 EA15  
KA01 NA02 NA05  
5K030 GA15 HB01 HB02 HC01 HC14  
HD01 HD06  
5K033 AA08 BA01 BA11 CB08 DA06  
DA11 DA13 DB10 DB18  
9A001 BB04 CC07 CC08 EE03 EE04  
JJ25 JJ27 KK56 LL03

## PRIOR ART DOCUMENTS

Application Number	
Your Ref.	
Our Ref.	102029US01
Applicant ( Assignee )	ONKYO CORPORATION
Filing Date	

### U.S. PATENT DOCUMENTS

	No.	Document No.	Name

### FOREIGN PATENT DOCUMENTS

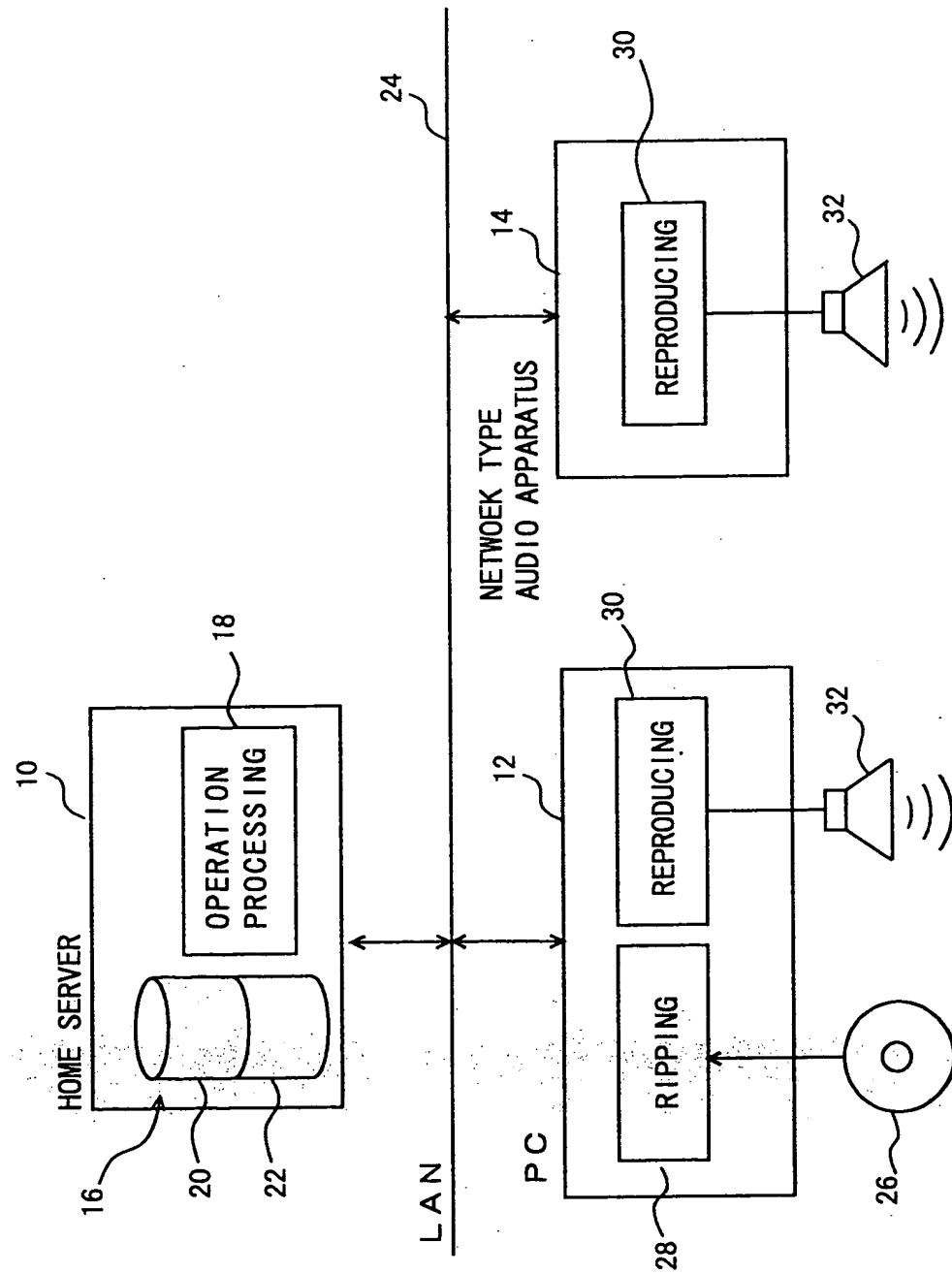
	No.	Document No.	Publication Date	Country	Translation	Equivalent
	1	2001-285283	Oct.12.2001	Japan	Abstract	No

### OTHER DOCUMENTS

--	--	--

\* discussed in the specification

FIG. 1



F I G. 2

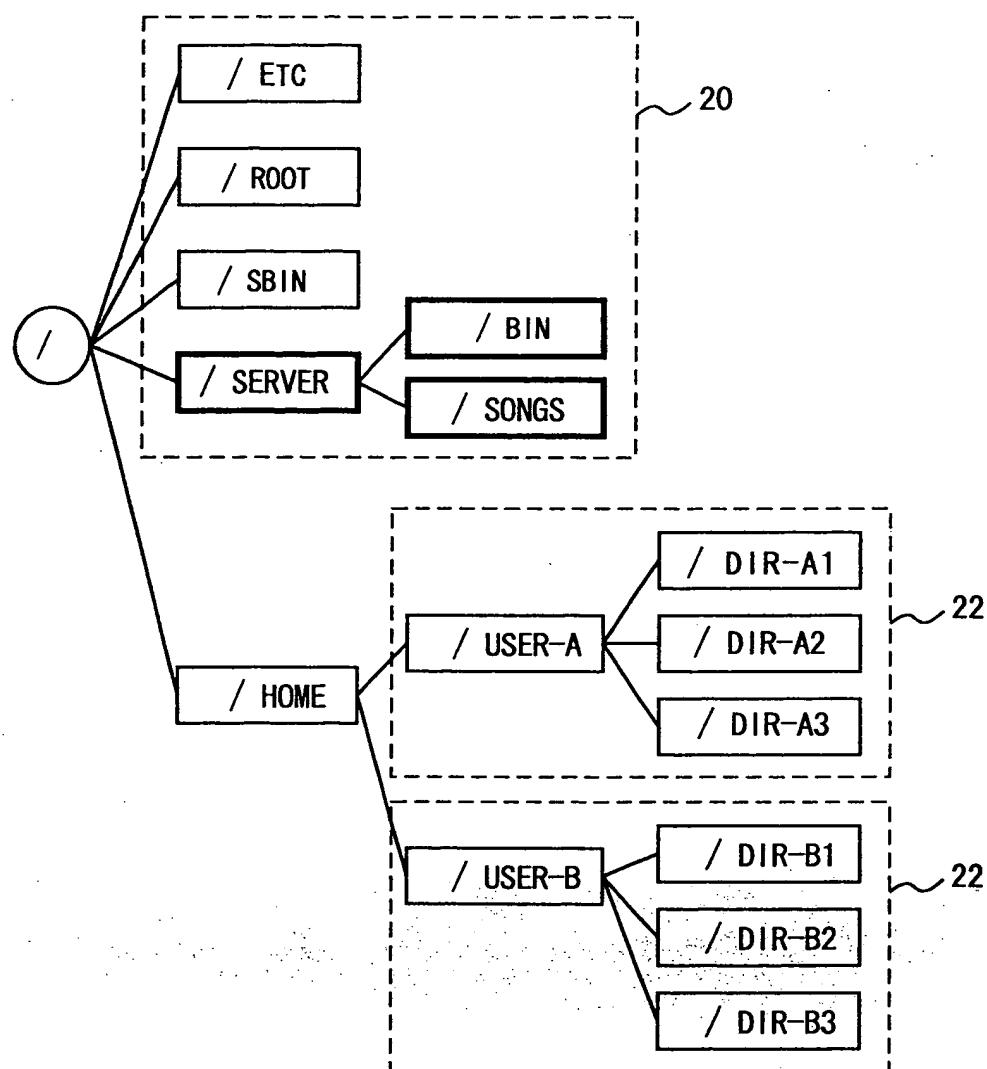


FIG. 3

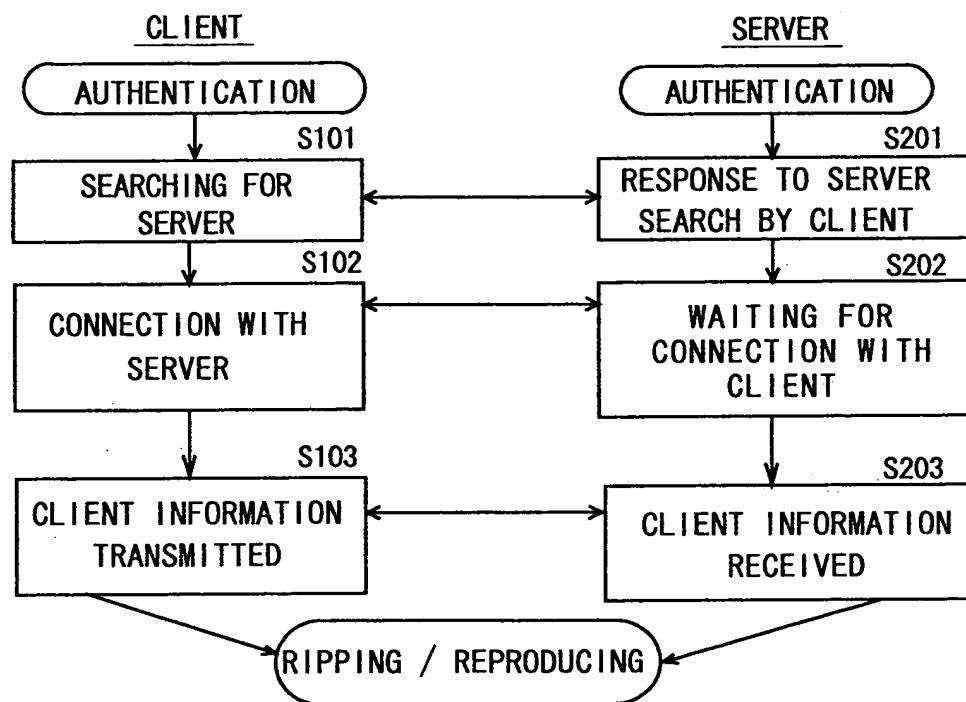


FIG. 4

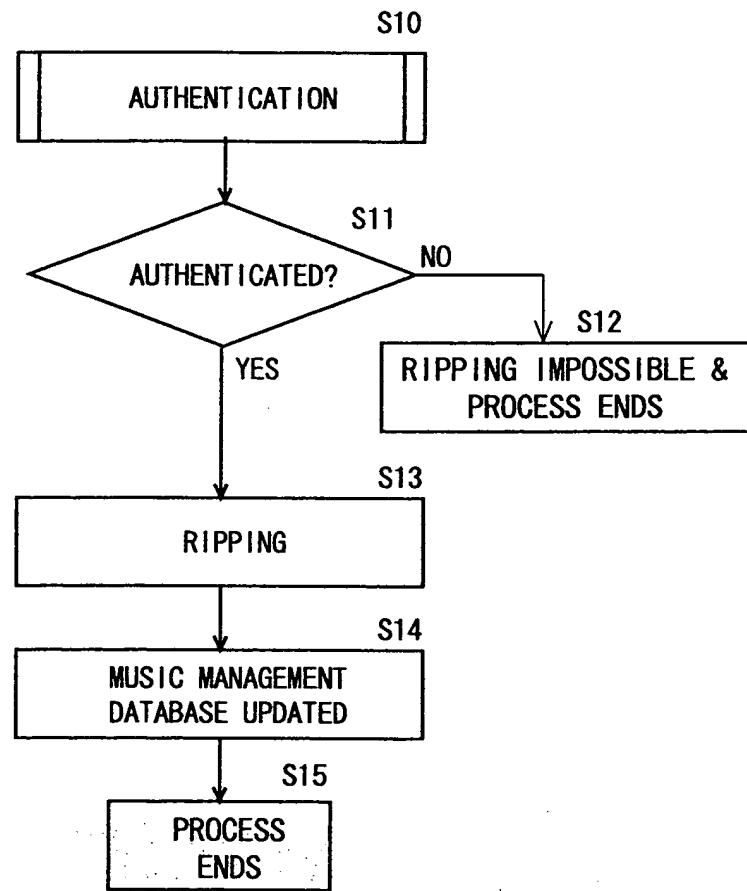


FIG. 5

